UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JONATHAN GABRIELLI, individually and on behalf of all others similarly situated,
 	
       Plaintiff,
 	
   v.
 	
 INSIDER, INC.,
 	
       Defendant.
	Case No. 1:24-cv-01566-ER
	
	 FIRST AMENDED CLASS ACTION COMPLAINT
	
	 JURY TRIAL DEMANDED

Plaintiff Jonathan Gabrielli ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his attorneys, makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to allegations specifically pertaining to himself and his counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. Insider, Inc. ("Defendant" or "Insider") owns and operates the website https://www.businessinsider.com (the "Website").

2. When users visit the Website, Defendant causes the Audiencerate Tracker to be installed on Website visitors' internet browsers. Defendant then uses the Audiencerate Tracker to collect IP addresses of visitors to the Website.

3. Because the Tracker captures Website visitors' "routing, addressing, or signaling information," the Tracker constitutes a "pen register" under Section 638.50(b) of the California Invasion of Privacy Act ("CIPA"). Cal. Penal Code § 638.50(b); *see also Greenley v. Kochava, Inc.*, 2023 WL 4833466 (S.D. Cal. July 27, 2023).

4. By installing and using the Tracker without Plaintiff's prior consent and without a court order, Defendant violated the CIPA § 638.51(a).

5.   Plaintiff brings this action to prevent Defendant from further violating the privacy rights of California residents, and to recover statutory damages for Defendant's violation of CIPA § 638.51.

PARTIES

6.   Plaintiff Gabrielli resides in Oakland, California and has the intent to remain there, and is therefore a citizen of California. Plaintiff Gabrielli was in California when he visited the Website.

7.   Defendant Insider, Inc. is a corporation incorporated in the State of Delaware, with its principal place of business in New York City, New York.

JURISDICTION AND VENUE

8.   This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(a) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00 exclusive of interest and costs, there are over 100 members of the putative class, and at least one class member is a citizen of a state different than Defendant.

9.   This Court has personal jurisdiction over Defendant because Defendant is headquartered in New York.

10.   Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant resides in this District.

FACTUAL ALLEGATIONS

I.   THE CALIFORNIA INVASION OF PRIVACY ACT

11.   The California Legislature enacted CIPA to protect certain privacy rights of California citizens. The California Legislature expressly recognized that "the development of new

devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

12.   As relevant here, CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

13.   A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

14.   A "trap and trace device" is a "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(b).

15.   In plain English, a "pen register" is a "device or process" that records *outgoing* information, while a "trap and trace device" is a "device or process" that records *incoming* information.

16.   Historically, law enforcement used "pen registers" to record the numbers of outgoing calls from a particular telephone line, while law enforcement used "trap and trace devices" to record the numbers of incoming calls to that particular telephone line. As technology advanced, however, courts have expanded the application of these surveillance devices.

17.   For example, if a user sends an email, a "pen register" might record the email address it was sent from, the email address the email was sent to, and the subject line—because this is the user's *outgoing* information. On the other hand, if that same user receives an email, a

"trap and trace device" might record the email address it was sent from, the email address it was sent to, and the subject line—because this is *incoming* information that is being sent to that same user.

18.   Although CIPA was enacted before the dawn of the Internet, "the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc.*, 2013 WL 5423918, at *21 (N.D. Cal. Sept. 26, 2013); *see also Greenley*, *supra*, 2023 WL 4833466, at *15 (referencing CIPA's "expansive language" when finding software was a "pen register"); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, [CIPA] Section 631(a) applies to Internet communications."). This accords with the fact that, "when faced with two possible interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection." *Matera v. Google Inc.*, 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

19.   Individuals may bring an action against the violator of any provision of CIPA—including CIPA § 638.51—for $5,000 per violation. Cal. Penal Code § 637.2(a)(1).

II.   DEFENDANT VIOLATES THE CALIFORNIA INVASION OF PRIVACY ACT

A.   The Tracker Is A "Pen Register"

20.   To make Defendant's Website load on a user's internet browser, the browser sends an "HTTP request" or "GET" request to Defendant's server where the relevant Website data is stored. In response to the request, Defendant's server sends an "HTTP response" back to the browser with a set of instructions. A general diagram of this process is pictured at Figure 1, which explains how Defendant's Website transmits instructions back to users' browsers in response to HTTP requests. *See* Figure 1.

Figure 1:
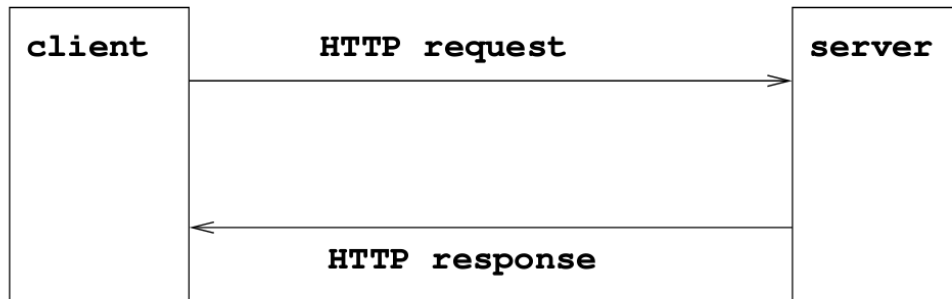
21.   The server's instructions include how to properly display the Website—*e.g.*, what images to load, what text should appear, or what music should play.

22.   In addition, the server's instructions cause the Tracker to be installed on a user's browser. The Tracker then causes the browser to send identifying information—including the user's IP address—to Audiencerate.

23.   The IP address is a unique identifier for a device, which is expressed as four sets of numbers separated by periods (*e.g.*, 192.168.123.132). The first two sets of numbers indicate what network the device is on (*e.g.*, 192.168), and the second two sets of numbers identify the specific device (*e.g.*, 123.132).

24.   Thus, the IP address enables a device to communicate with another device—such as a computer's browser communicating with a server—and the IP address contains geographical location.

25.   Through an IP address, the specific device's state, city, and zip code can be determined.

26.   Much like a telephone number, an IP address is a unique numerical code associated with a specific internet-connected device. Thus, knowing a user's IP address—and therefore

geographical location—"provide[s] a level of specificity previously unfound in marketing."[1]

27.   An IP address allows advertisers to (i) "[t]arget [customers by] countries, cities, neighborhoods, and … postal code"[2] and (ii) "to target specific households, businesses[,] and even individuals with ads that are relevant to their interests."[3] Indeed, "IP targeting is one of the most targeted marketing techniques [companies] can employ to spread the word about [a] product or service"[4] *because* "[c]ompanies can use an IP address … to personally identify individuals."[5]

28.   For example, businesses who are trying to reach college-aged demographics can target devices on college campuses by sending advertisements to IP addresses associated with college-wide Wi-Fis.[6] Or, for a job fair in specific city, companies can send advertisements to only those in the general location of the upcoming event.[7]

29.   In addition to "reach[ing] their target audience with greater precision," businesses are incentivized to use a customer's IP address because it "can be more cost-effective than other forms of advertising."[8] "By targeting specific households or businesses, businesses can avoid

---

[1] *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA, https://www.accudata.com/blog/ip-targeting/ (last visited April 24, 2024).

[2] *Location-based Targeting That Puts You in Control*, CHOOZLE, https://choozle.com/geotargeting-strategies/ (last visited April 24, 2024).

[3] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf.

[4] *IP Targeting: Understanding This Essential Marketing Tool*, *supra* note 1.

[5] Trey Titone, *The future of IP address as an advertising identifier*, AD TECH EXPLAINED (May 16, 2022), https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/.

[6] *See*, *e.g.*, *IP Targeting: Understanding This Essential Marketing Tool*, *supra* note 1.

[7] *See*, *e.g.*, *Personalize Your Website And Digital Marketing Using IP Address*, GEOFLI, https://geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-marketing-campaigns (last visited April 24, 2024).

[8] Williams, *supra* note 3.

wasting money on ads that are unlikely to be seen by their target audience."[9]

30.   In addition, "IP address targeting can help businesses to improve their overall marketing strategy."[10] "By analyzing data on which households or businesses are responding to their ads, businesses can refine their targeting strategy and improve their overall marketing efforts."[11]

31.   As alleged below, Defendant installs the Tracker on the user's browser for marketing and analytics purposes, and the Tracker collect information—users' IP addresses—that identifies the outgoing "routing, addressing, or signaling information" of the user. Accordingly, the Tracker is a "pen register."

1.   *Audiencerate Tracker*

32.   Audiencerate LTD ("Audiencerate") is a software-as-a-service company that develops the Audiencerate Tracker, which it provides to website owners, like Defendant, for a fee.

33.   According to Audiencerate, it "enable[s] data-driven advertising via [its] proprietary technology and platforms."[12]

34.   "One side of [Audiencerate's] business is dedicated to helping data owners monetize their data and license audiences in the world's largest programmatic media buying marketplaces. The other side provides targeting data to marketers, enabling them to model and target audiences with more complexity and sophistication."[13]

---

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] AUDIENCERATE, https://www.audiencerate.com/ (last visited Feb. 26, 2024).

[13] *AWS Enables Audiencerate to Process Over a Billion Requests per Week*, AWS (2020), https://aws.amazon.com/solutions/case-studies/audiencerate-case-study/.

35.   Audiencerate uses its Tracker to receive, store, and analyze data collected from website visitors, including visitors of Defendant's Website.

36.   The first time a user visits Defendant's Website, the user's browser sends an HTTP request to Defendant's server, and Defendant's server sends the HTTP response. This response also includes directions to install the Audiencerate Tracker on the user's browser.   The Audiencerate Tracker, in turn, instructs the user's browser to send the user's IP address to Audiencerate.

37.   Moreover, Audiencerate stores a cookie in the user's browser cache. When the user subsequently visits Defendant's Website, the Audiencerate Tracker instructs the user's browser to send the user's IP address through the cookie. *See* Figure 2.

Figure 2:
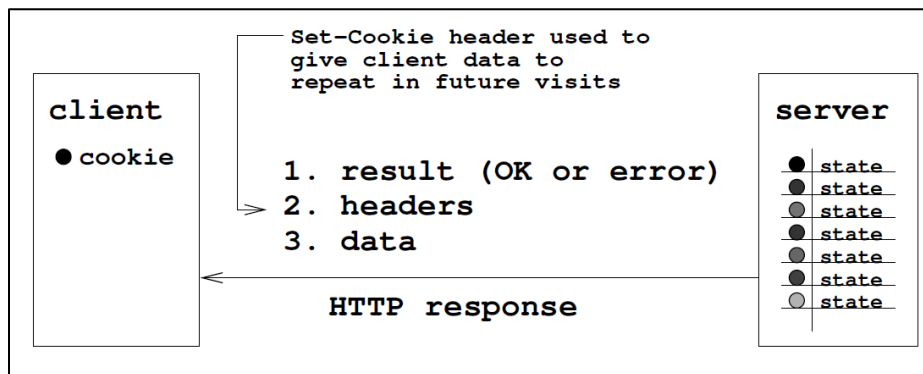
38.   If the user clears his or her cookies, then the user wipes out the Audiencerate Tracker from its cache. Accordingly, the next time the user visits Defendant's Website the process begins over again: (i) Defendant's server installs the Audiencerate Tracker on the user's browser, (ii) the Audiencerate Tracker instructs the browser to send Audiencerate the user's IP address, (iii) the Audiencerate Tracker stores a cookie in the browser cache, and (iv) Audiencerate will continue to receive the user's IP address on subsequent Website visits with the cookie transmission. *See* Figure 3.

Figure 3:
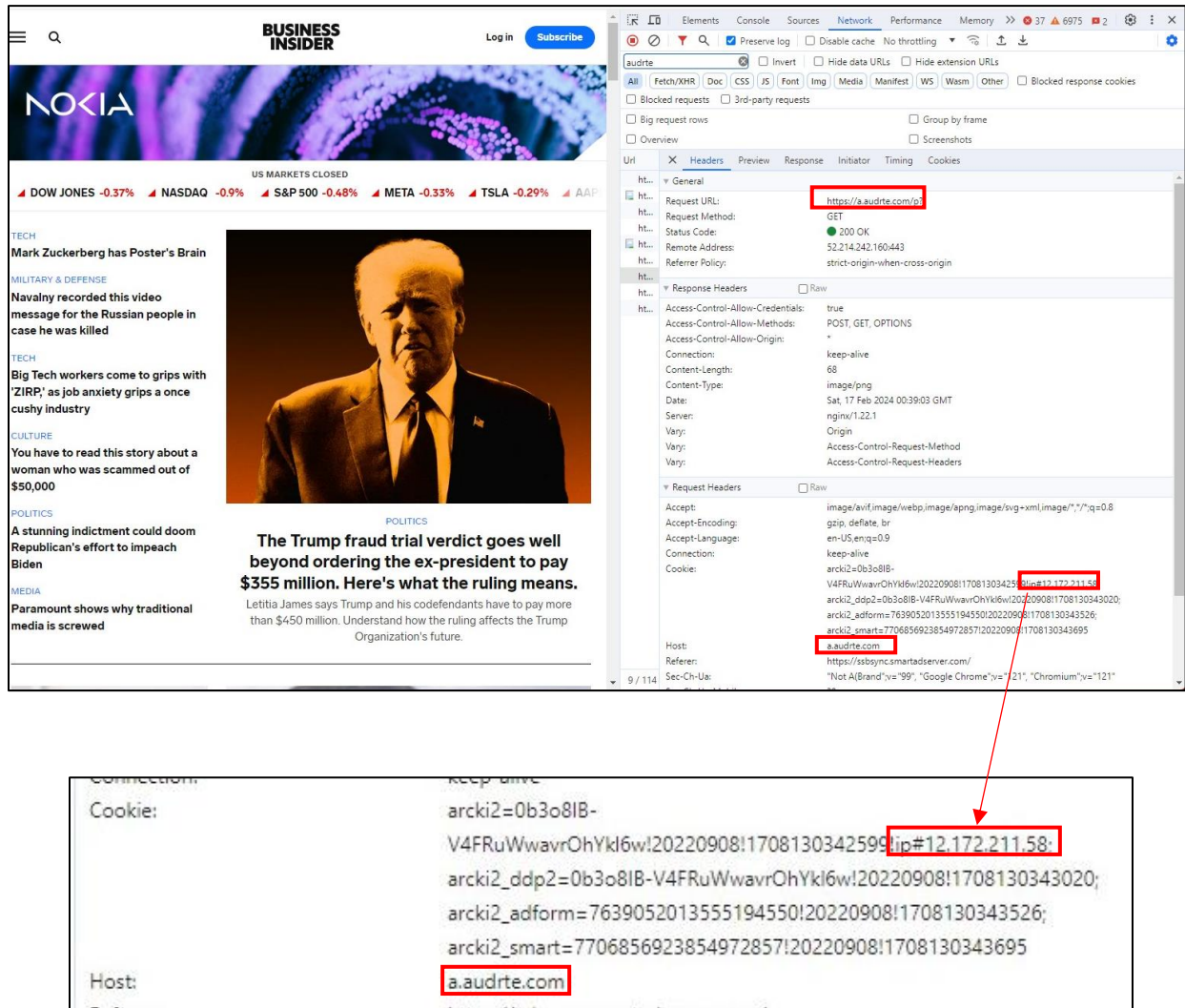
39.   The Audiencerate Tracker is at least a "process" because it is "software that identifies consumers, gathers data, and correlates that data." *Greenley*, *supra*, 2023 WL 4833466, at *15.

40.   Further, the Audiencerate Tracker is a "device" because "in order for software to work, it must be run on some kind of computing device." *James*, *supra*, 2023 WL 7392285, at *13.

41.   Because the Audiencerate Tracker captures the outgoing information—the IP address—from visitors to websites, it is a "pen register" for the purposes of CIPA§ 638.50(b).

9

B.   Defendant Installed And Used The Tracker On Plaintiff's And Users' Browsers Without Prior Consent Or A Court Order

42.   Defendant Insider, Inc. owns and operates the Business Insider Website. Business Insider is a "digital business news site" that focuses on "cover[ing] the people, companies, and ideas changing our world."[14]

43.   When companies build their websites, they install or integrate various third-party scripts into the code of the website in order to collect data from users or perform other functions.[15]

44.   Oftentimes, third-party scripts are installed on websites "for advertising purposes."[16]

45.   Further, "[i]f the same third-party tracker is present on many sites, it can build a more complete profile of the user over time."[17]

46.   Defendant has long incorporated the code of this Tracker into the code of its Website, including when Plaintiff and other users visited the Website. Thus, when Plaintiff visited the Website, the Website caused the Tracker to be installed on Plaintiff's and other users' browsers.

47.   As outlined above, when a user visits the Website, the Website's code—as programmed by Defendant—installs the Tracker onto the user's browser.

48.   Upon installing the Tracker on its Website, Defendant uses the Tracker to collect the IP address of visitors to the Website, which is used by Audiencerate to provide services to

---

[14] INSIDER, INC., https://www.insider-inc.com/#home-brand-bi (last visited Feb. 25, 2024).

[15] *See Third-party Tracking*, PIWIK, https://piwik.pro/glossary/third-party-tracking/ (last visited Jan. 19, 2024) ("Third-party tracking refers to the practice by which a tracker, other than the website directly visited by the user, traces or assists in tracking the user's visit to the site. Third-party trackers are snippets of code that are present on multiple websites. They collect and send information about a user's browsing history to other companies…").

[16] *Id.*

[17] *Id.*

Defendant and its other clients, including targeted advertisements and website analytics.

49.   At no time prior to the installation and use of the Tracker on Plaintiff's and Class

Members' browsers, or prior to the use of the Tracker, did Defendant procure Plaintiff's and Class

Members' consent for such conduct. Nor did Defendant obtain a court order to install or use the

Tracker.

C.   Defendant's Conduct Constitutes An Invasion Of Plaintiff's And Class Members' Privacy

50.   The collection of Plaintiff's and Class Members' personally identifying, non-

anonymized information through Defendant's installation and use of the Tracker constitutes an

invasion of privacy.

51.   As alleged herein, the Tracker is designed to analyze Website data and marketing

campaigns, conduct targeted advertising, and boost Defendant's revenue, all through their

surreptitious collection of Plaintiff's and Class Members' data.

1.   Defendant Discloses User's Data To Audiencerate For The Purpose Of Marketing, Advertising, And Analytics

52.   Audiencerate is a data platform that "enable[s] data-driven advertising via [its]

proprietary technology and platforms" for marketing, advertising, and analysis purposes.[18]

53.   Companies such as Defendant share their users' data with Audiencerate through

"daily synchronization" via the Audiencerate Tracker.[19] Audiencerate claims to anonymize the

data and organize it into segments.[20] Then, companies use the segmented data to run targeted
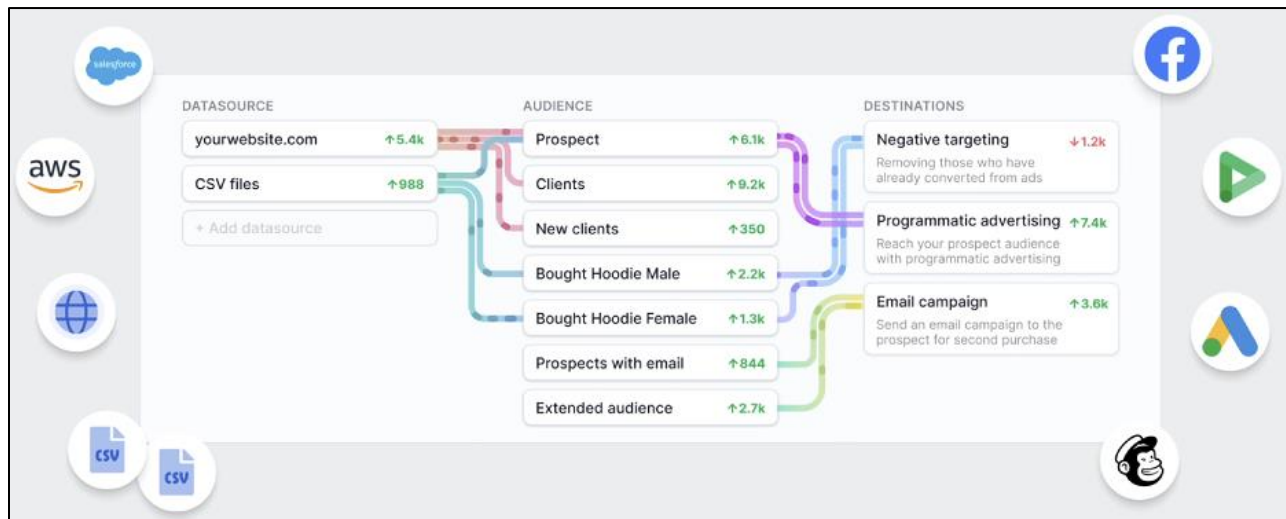
---

[18] AUDIENCERATE, https://www.audiencerate.com/ (last visited Jan. 4, 2024).

[19] *Id.*

[20] *Product Overview*, AUDIENCERATE, https://app.audiencerate.com/doc/home (last visited Jan. 3, 2024).

campaigns and perform data analysis through Audiencerate's platform.[21] *See* Figure 4.

Figure 4:

54.   In addition to helping companies make better use of their own customer data, Audiencerate helps companies *sell* their customers' data to further "monetize data."[22]

55.   In order to perform the functions listed above, Audiencerate needs to collect data that identifies a particular user. This is why Audiencerate collects IP addresses: it allows Audiencerate to segment users in order to run targeted campaigns and perform data analysis.

56.   In other words, companies like Defendant are collecting users' data and sending it to Audiencerate for a profit, whether it is by optimizing marketing campaigns or by purely selling the data.

III.   PLAINTIFF'S EXPERIENCE

57.   Plaintiff has visited the Website multiple times—including as long ago as March 2020 and as recently as December 2023—on his desktop browser.

---

[21] *Id.*

[22] *Audiencerate partnership sees Sirdata integrated on Adform marketplace for the first time*, SIRDATA (Dec. 10, 2020), https://news.sirdata.com/en/press-release-audiencerate-sirdata-partnership/.

58.   When Plaintiff visited the Website, the Website's code—as programmed by Defendant—caused the Tracker to be installed on Plaintiff's browser.   Defendant and Audiencerate then used the Tracker to collect Plaintiff's IP address. *See* Figure 5 (Audiencerate Tracker).

Figure 5:
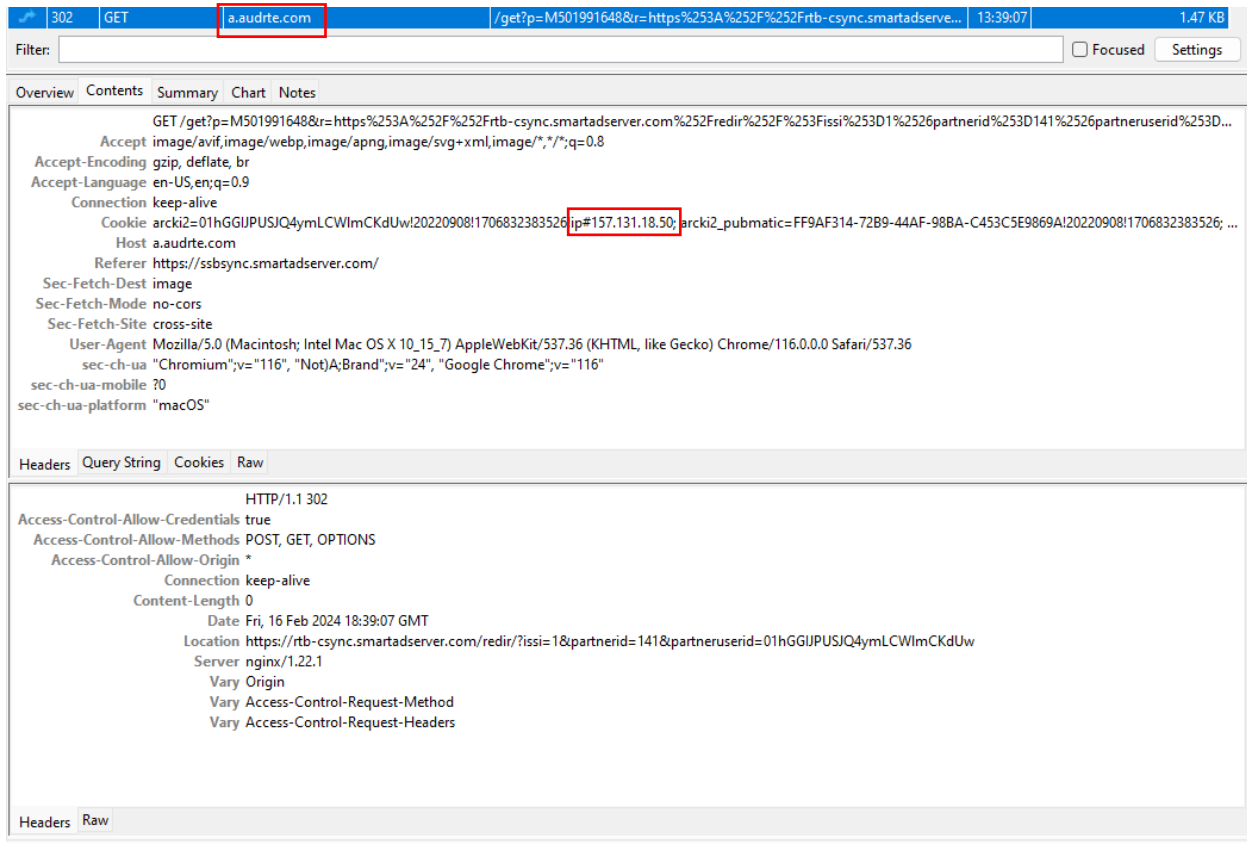
59.   Defendant and Audiencerate used the information collected by the Tracker to analyze Website data and marketing campaigns, conduct targeted advertising, and ultimately boost Defendant's and advertisers' revenue.

60.   Plaintiff did not provide his prior consent to Defendant to install or use the Tracker on Plaintiff's browser.

61.   Defendant did not obtain a court order before installing or using the Tracker.

62.   Plaintiff has, therefore, had his privacy invaded by Defendant's violations of CIPA § 638.51(a).

CLASS ALLEGATIONS

63.   Pursuant to Fed. R. Civ. P. 23(a) and 23(b)(3), Plaintiff seeks to represent a class defined as all California residents who accessed the Website in California and had their IP address collected by the Tracker (the "Class").

64.   The following people are excluded from the Class: (i) any Judge presiding over this action and members of her or her family; (ii) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or their parents have a controlling interest (including current and former employees, officers, or directors); (iii) persons who properly execute and file a timely request for exclusion from the Class; (iv) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (v) Plaintiff's counsel and Defendant's counsel; and (vi) the legal representatives, successors, and assigns of any such excluded persons.

65.   **Numerosity:** The number of people within the Class is substantial and believed to amount to thousands, if not millions of persons. It is, therefore, impractical to join each member of the Class as a named plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Class is ascertainable and identifiable from Defendant's records.

66.   **Commonality and Predominance:** There are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions

affecting only individual members of the Class. These common legal and factual questions, which

do not vary between members of the Class, and which may be determined without reference to the

individual circumstances of any Class Member, include, but are not limited to, the following:

> (a)   Whether Defendant violated CIPA § 638.51(a);
>
> (b)   Whether the Tracker is a "pen register" pursuant to Cal. Penal Code §§ 638.50(b);
>
> (c)   Whether Defendant sought or obtained prior consent—express or otherwise—from Plaintiff and the Class;
>
> (d)   Whether Defendant sought or obtained a court order for its use of the Tracker; and
>
> (e)   Whether Plaintiff and members of the Class are entitled to actual and/or statutory damages for the aforementioned violations.

67.   **Typicality:** The claims of the named Plaintiff are typical of the claims of the Class

because the named Plaintiff, like all other members of the Class Members, visited the Website and

had his IP address collected by the Trackers, which were installed and used by Defendant.

68.   **Adequate Representation:** Plaintiff is an adequate representative of the Class

because his interests do not conflict with the interests of the Class Members he seeks to represent,

he has retained competent counsel experienced in prosecuting class actions, and he intends to

prosecute this action vigorously. The interests of members of the Class will be fairly and

adequately protected by Plaintiff and his counsel.

69.   **Superiority:** The class mechanism is superior to other available means for the fair

and efficient adjudication of the claims of members of the Class. Each individual member of the

Class may lack the resources to undergo the burden and expense of individual prosecution of the

complex and extensive litigation necessary to establish Defendant's liability. Individualized

litigation increases the delay and expense to all parties and multiplies the burden on the judicial

system presented by the complex legal and factual issues of this case. Individualized litigation

also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSES OF ACTION

COUNT I
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 638.51(a)

70.   Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

71.   Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

72.   CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

73.   A "pen register" is "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

74.   The Tracker is a "pen register" because it is a "device or process" that "capture[d]" the "routing, addressing, or signaling information"—the IP address—from the electronic communications transmitted by Plaintiff's and the Class's computers or smartphones. Cal. Penal Code § 638.50(b).

75.   At all relevant times, Defendant installed the Tracker—which is a pen register—on Plaintiff's and Class Members' browsers, and used the Tracker to collect Plaintiff's and Class Members' IP addresses.

76.   The Tracker does not collect the content of Plaintiff's and the Class's electronic communications with the Website. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1008 (9th Cir. 2014) ("IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication…") (cleaned up).

77.   Plaintiff and Class Members did not provide their prior consent to Defendant's installation or use of the Tracker.

78.   Defendant did not obtain a court order to install or use the Tracker.

79.   Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by Defendant's violations of CIPA § 638.51(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 638.51(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a)   For an order certifying the Class, naming Plaintiff as the representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;

(b)   For an order declaring that Defendant's conduct violates the statutes referenced herein;

(c)   For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d)   For statutory damages of $5,000 for each violation of CIPA § 638.51(a);

(e)   For pre- and post-judgment interest on all amounts awarded;

(f)   For an order of restitution and all other forms of equitable monetary relief; and

(g)   For an order awarding and the Class their reasonable attorney's fees and expenses and costs of suit.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of any and all issues in this action so triable of right.

Dated: June 11, 2024   Respectfully submitted,

                                                     BURSOR & FISHER, P.A.

                                                     By: */s/ Yitzchak Kopel*
                                                           Yitzchak Kopel

                                                     Yitzchak Kopel
                                                     Alec M. Leslie
                                                     Max S. Roberts
                                                     1330 Avenue of the Americas, 32nd Floor
                                                     New York, NY 10019
                                                     Telephone: (646) 837-7150
                                                     Facsimile: (212) 989-9163
                                                     Email: ykopel@bursor.com
                                                                 aleslie@bursor.com
                                                                 mroberts@bursor.com

                                                     Attorneys for Plaintiff